2011

Strategies for Combating Dark Networks

Roberts, Nancy

Journal of Social Structure, JoSS Article: Vol. 12
http://hdl.handle.net/10945/41260

Journal of Social Structure

JoSS Article: Volume 12

Strategies for Combating Dark Networks

Nancy Roberts
Department of Defense Analysis, Naval Postgraduate School, Monterey, CA 93943
nroberts@nps.edu

Sean F. Everton
Department of Defense Analysis, Naval Postgraduate School, Monterey, CA 93943
sfeverto@nps.edu

Abstract

Our goal in this paper is to explore two generic approaches to disrupting dark networks: kinetic and non-kinetic. The kinetic approach involves aggressive and offensive measures to eliminate or capture network members and their supporters, while the non-kinetic approach involves the use of subtle, non-coercive means for combating dark networks. Two strategies derive from the kinetic approach: Targeting and Capacity-building. Four strategies derive from the non-kinetic approach: Institution-Building, Psychological Operations, Information Operations and Rehabilitation. We use network data from Noordin Top's South East Asian terror network to illustrate how both kinetic and non-kinetic strategies could be pursued depending on a commander's intent. Using this strategic framework as a backdrop, we strongly advise the use of SNA metrics in developing alterative counter-terrorism strategies that are context-dependent rather than letting SNA metrics define and drive a particular strategy.

Key Words

Dark networks, counter-terrorism, counter-insurgency, strategy

Acknowledgements

We would like to thank JoSS editor James Moody and two anonymous reviewers for their careful reading of our paper. Their thoughtful comments greatly enhanced the final version of this paper. .

Introduction

Tracking dark networks, i.e., illegal and covert networks (Raab & Milward, 2003), has a relatively long history. Considerable effort and energy have gone into gathering and analyzing data to flesh out networks' relational structures and members' locations. Earliest formal efforts can be traced backed to WWII when a branch of cryptology—Traffic Analysis, also known as communication link analysis—focused on the structures and operations of communication systems by determining who called whom, in what order, at what time and for how long (van Meter, 2001). In the post WWII era, the British MI5 internal security service used traffic analysis to combat the IRA in the 1980s and 1990s. It continues to be used by law-enforcement agencies including the U.S. Defense Intelligence Agency (DIA) Office of National Drug Control Policy (van Meter, 2001). Another example, the Village Survey Method, introduced by Ralph McGehee in Thailand in the mid sixties, connected family and community ties to identify the clandestine structure of local and regional Communist Party membership and arms training (van Meter, 2001).

A number of more recent examples are worth noting.[1] Valdis Krebs' (2001) mapping of the social network of the nineteen 9-11 hijackers who converged on leader, Mohamed Atta, helped popularize the use of social network analysis (SNA) as a tool for tracking dark networks. Jose' Rodriguez (2005) conducted a similar analysis to map the March 11th 2004 Madrid bombing, and Marc Sageman (2004) collected biographies of 172 Islamic terrorist operatives affiliated with the Salafi global jihad led by al Qaeda for the purpose of studying terrorist social networks operating throughout the world. And the Army's Able Danger project, which some analysts referred to as the "Kevin Bacon Game," sought to map al Qaeda by "identifying linkages and patterns in large volumes of data" (Keefe, 2006).

Various centers also collect and analyze data on world-wide dark networks. For example, the National Counterterrorism Center, the U.S. Government's central repository of information on international terrorists, has more than 540,000 names of individuals, with an estimated 450,000 separate identities due to the use of aliases and name variants.[2] The University of Arizona's Artificial Intelligence Center, specifically its Dark Web Terrorism Research Program, has developed an extensive database of news articles and Web pages from various Web sites, search engines and news portals to study the international terrorism (Jihadist) phenomenon. Its aim is to collect "all" web content generated by terrorist groups to include web sites, fora, chat rooms, blogs, social networking sites, videos, virtual worlds, etc.[3]

With all the interest devoted to collecting information on dark networks, it is surprising that so little attention is paid to exploring strategies for their disruption. Strategies for combating terror networks are not well documented in the literature and references to multiple strategies are rare.[4] The Davis and Sisson (2009) study is an exception, but it only offers a limited discussion of alternative strategies based on input from RAND experts. To our knowledge, no comprehensive or systematic study exists that identifies the range of strategic options available to combat terrorism, nor have we been able to find any assessment that considers the costs, benefits or trade-offs that have to be made when selecting a specific strategy. As Lum et. al. (2006:3) have noted, "there is almost a complete absence of high quality scientific evaluation evidence on counter-terrorism strategies," and what evidence exists does not show a positive relationship between the strategy and results. In fact, some counterterrorism interventions may even increase the likelihood of terrorism and terrorism-related harm (C. Lum, et al., 2006).

Furthermore, with the exception of RAND's study of US grand strategies (Lempert, et al., 2008), we find no research that compares and contrasts alternative strategies, especially at the operational level, and none examine strategies with a view toward balancing their potential gains with their likely potential costs. Judging by the literature on the subject, it appears axiomatic that once a dark network's contours and members have been discovered, one is supposed to capture and eliminate designated high value targets.[5] While we agree that pursuing high value targets is one option to consider, other options exist and

arguable may offer better alternatives when considering costs, human lives, and the consequences for affected communities. Recent speculation in fact suggests that direct attacks may even worsen the terrorist threat (Schmitt & Perlez, 2009). As General Flynn and his coauthors (2010:8) warn in the much-publicized report, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan*, "lethal targeting alone will not help U.S. and Allied forces win in Afghanistan." In fact, "merely killing insurgents usually serves to multiply enemies rather than subtract them." Clearly research on strategies to counter dark networks is needed. As social scientists it is incumbent upon us to investigate the consequence of counter-terrorism strategies and ascertain what effects they are having. Are they, as implied by General Flynn and others, actually increasing rather than decreasing the level of violence? If this is the case, does the violence increase with all counter-terror strategies or only those that are enemy-focused rather than population-focused? To address this question, we first need to provide a conceptual framework to distinguish among the different types of counter-terror strategies. This is our charge in this article. Follow-on research will explore the association between counter-terror strategies and levels of violence and the conditions under which violence may increase or decrease.

We begin this effort by distinguishing between two general approaches to countering dark networks: the Kinetic and Non-Kinetic approaches.[6] The kinetic approach pursues aggressive, offensive measures to eliminate or capture network members and their supporters and employs such things as bombs and bullets to pursue the campaign. It can be further subdivided it into two types: action directed by the U.S. military and action directed by the host-nation military. By contrast, the non-kinetic approach employs neither bombs nor bullets but instead uses non-coercive means to counter networks and impair a combatant's will to fight. It includes such activities as the reconstruction of war-torn areas, intelligence and psychological operations to win over the "hearts and minds" of local populations, and efforts at terrorist rehabilitation.[7] Like the kinetic approach, it too can be U.S. or host-nation led.

Our goal in this paper is to illustrate how social network analysis can be a useful tool to flesh out the strategic options within both the kinetic and non-kinetic approaches. We acknowledge the use of social network analysis for such a purpose has its challenges. Three are particularly noteworthy. First, data on insurgencies and terrorists can be difficult to collect and likely incomplete (Borgatti, Carley, & Krackhardt, 2006; Krebs, 2001; Sparrow, 1991). Pursuing strategies on the basis of incomplete data would be dangerous and irresponsible. We agree. In our experience, however, there is a surprising amount of detailed information on some terror groups in the open-source literature. Our challenge has not been in finding data, but sorting through the tremendous amount that currently exists and is growing exponentially. Moreover, the "Cold War notion that open-sourced information is 'second class' is a dangerous, outmoded cliché" (Flynn, et al., 2010:23). As former Director of the Defense Intelligence Agency, Lieutenant General Samuel V. Wilson put it (cited in Flynn, et al., 2010:23): "Ninety percent of intelligence comes from open sources. The other 10 percent, the clandestine work, is just the more dramatic. The real intelligence hero is Sherlock Holmes, not James Bond." Consequently, analysts need to "embrace open-source, population-centric information as the lifeblood of their analytical work" (Flynn, et al., 2010:23).

Secondly, critics have challenged the use of social network analysis for military purposes. Their complaints center on the use of social network analysis for targeting purposes. We share their concerns. At the very least, as noted above, lethal targeting may very well increase the level of violence rather than reduce it. Furthermore, emphasis on kinetic operations neglects or minimizes the use of social network analysis for rebuilding, reconstructing and rehabilitating societies. We believe a discussion of the full range of counter-terror strategies is well past due and social network analysis is an excellent vehicle to flesh out other applications for its use.

Thirdly, using social network analysis to generate strategic options should not be confounded with the use of social network analysis for decision-making. Strategic choice depends on a range of issues—knowledge of context, assessment of risks, costs, and potential for unintended consequences to name just a few (Moody, 2005). Social network analysis is not, nor should it be, a substitute for other critical elements in the decision process. It certainly can inform decisions, but it should not determine them. Thus, we emphasize the use of social network analysis for the generation of alternative strategies, not their selection.

Keeping these challenges in mind, our goal in this paper is to demonstrate the broad applications of social network analysis in crafting alternative strategies to counter terror and insurgencies.[8] Our focus and examples will be strategies at the operational level. We do not assume that the strategies are mutually exclusive although some are likely to form a more compatible set than others.

Strategies in Counter-Terrorism Operations

Of the two generic approaches to combating terrorism, the kinetic approach receives greater visibility. The capture of high-value targets attracts headlines and engenders popular support. The subtlety and long-term duration of the non-kinetic approach, as well as the patience and skill to implement it, receives far less attention. Special Operations Commander, Admiral Eric T. Olson, who was appointed to the post in July 2007, has been trying to shift the emphasis away from the high-profile raids that are the hallmark of kinetic action and characteristic of the early years of U.S. anti-terrorism efforts. Instead, he has been stressing the training of friendly militaries to better fight terrorism and violent separatists within their own borders as well as the use of more non-kinetic actions. While he acknowledges that kinetic action may be "urgent and necessary," it is his belief that it is "not decisive. It is a holding action that buys time for the indirect approach to have its decisive effect."[9] Because of the importance of these two counterterrorism approaches, we explore their perspectives and strategies in greater depth below.

Kinetic Approach

A proactive and aggressive approach, kinetic action targets enemy combatants and their supporters to neutralize, capture or eliminate them. We term the strategies that derive from it as *the targeting and capacity-building strategies*. The former is U.S. led, while the latter is host-nation led. Both can be pursued at the individual, group, and organizational (i.e., institutional) levels. However, as we shall see in the next section, no matter what the level of analysis or whether it is U.S. led or host-nation led, strategies of disruption follow a similar pattern. They either involve the removal of central nodes or brokers, or they involve the breaking of key ties or links among individuals, groups, or organizations.

Targeting

Person-Targeting: When individuals are this strategy's focus, such as the apprehension of Saddam Hussein, Abu Musab al-Zarqawi, or key al Qaeda and Taliban leaders in Afghanistan, the US military describes the operation as man-hunting (Marks, Meer, & Nilson, 2005).

Group-Targeting: When teams, groups, or a particular subset of a terror network is the focus, we describe the operation as group-targeting. Examples include the round-up of specific groups fashioning IEDs in Iraq (Peter, 2008), the disruption of the Syrian recruitment network bringing jihadists into Iraq (Felter & Fishman, 2007), and the shut-down of the financial network supporting the Indonesia-based Jemaah Islamiyah (JI) (Abuza, 2003).

Organization-Targeting: When organizations are the focus of strategies that seek to limit their activities or shut them down, we describe the operations as organization-targeting. Examples include Malaysia's successful effort to close down Luqmanul Hakiem, a jihadist religious boarding school, (Rabasa, 2005) and its closure of the Al-Qaeda-linked Islamic NGO, Pertubuhan al Ehasan in 2002 (Abuza, 2003).

Capacity-Building

We refer to the strategy where the U.S. military works "through, by, and with" indigenous forces to build their capacity to conduct effective targeting operations against common enemies as capacity-building. Here, the focus is on training and advising others' security forces to become a professional force rather than pursuing a U.S.-led security strategy (Fridovich & Krawchuk, 2007). Although some U.S. military references treat capacity-building as an example of the indirect approach,[10] we prefer to characterize it as kinetic because of its use of aggressive, coercive tactics. Operation Enduring Freedom in the Philippines in 2002 was one such example. Special Operation Command forces deployed to Basilan, a southern island, to advise and train the Armed Forces of the Philippines (Fridovich & Krawchuk, 2007; Krawchuk, ND; Wilson, 2006). The outcome of this effort was to reduce the threat posed by the Abu Sayyaf Group (ASG). By 2005, the armed strength of the ASG fell from an estimated 1,000 in 2002 to somewhere between 200 and 400 in 2005 (T. Lum & Niksch, 2006; updated 2009). Like the targeting strategy, capacity-building can involve *person-, group- or organization-targeting*.

Non-Kinetic Approach

The non-kinetic approach is a less aggressive means to counter dark networks. It involves a more subtle and patient application of power by seeking to undermine terror networks "more through cooperation and collaboration with partners than through unilateral American action, more with the diplomatic and economic tools of national power than with the military, stressing inspiration rather than prescription" (Brimley & Singh, 2008:313). One can trace its roots back to the ancient Chinese theorist Sun Tzu, who advised that direct methods were used for joining battle, but indirect methods were used to secure victory (Brimley & Singh, 2008:316). T.E. Lawrence and the strategist Lindell Hart echoed similar themes in the 20th century, and the essence of their views is reflected in the latest Quadrennial Defense review:

> To succeed in (irregular warfare), the United States must often take an indirect approach, building up and working with others. The indirect approach seeks to unbalance adversaries physically and psychologically, rather than attacking them where they are the strongest or in the manner they expect to be attacked (quoted in Brimley & Singh, 2008:316).[11]

Like the kinetic approach, the non-kinetic approach can be U.S. or host-nation led, depending on resources and capabilities. The intent is to secure the population's safety and support and undermine the enemy's influence and control. There are multiple means to accomplish these efforts: through institution-building, psychological operations (PsyOp), information operations (IO) and rehabilitation.

Institution-Building

This strategy promotes reconstruction in war-torn communities. It requires the active involvement of Civil Affairs forces that provide humanitarian and civic assistance and work in tandem with inter-government and inter-agency partners in the reconstruction process. The emphasis is on building healthy host-government institutions of governance, rule of law, and economic development (Fridovich & Krawchuk, 2007).

Psychological Operations (PsyOp)

This strategy involves the dissemination of information for the purpose of influencing the emotions, perceptions, attitudes, objective reasoning, and ultimately the behavior of foreign nationals (individuals, groups, organizations, governments) so that they are more aligned with US goals and objectives during times of conflict and peace (U.S. Special Operations Command, 2003). Psychological operations are also employed to counter adversary propaganda and to sow disaffection and dissidence among adversaries to reduce their will to fight and ultimately to induce their surrender.

One example is the UK's plan to split the Taliban from within by securing the defection of its senior members and a large number of their supporters. It follows from Gordon Brown's decision to put much greater focus on courting "moderate" Taliban leaders and "tier-two" foot soldiers who fight more for money and a sense of tribal loyalty than for the Taliban's ideology[12] as well as from the U.S.' consideration of a divide-and-conquer strategy to peel away some lower-level members of the Taliban and win back the population (Cooper, 2009). The intent is to alter local jihadists' perception that partnering with al Qaeda enables them to achieve their political goals. PsyOp approaches also include deception tactics that attempt to turn terrorists or sub-groups within an organization against each other.

Information Operations (IO)

This strategy uses integrated employment of electronic warfare and computer network operations to combat terrorism.[13] Electric Warfare refers to any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the adversary. Computer Network Operations is one of the latest capabilities developed in support of military operations and stems from the increasing use of networked computers and supporting IT infrastructure systems by military and civilian organizations. Along with Electronic Warfare, it is used to attack, deceive, degrade, and disrupt information operations capabilities and to deny, exploit, and defend electronic information and infrastructure. Examples include the disruption of fund transfers, the monitoring of charitable donations, the detection of money laundering, black market activity and the drug trade. Activities also include interventions to compromise terrorists' cell phone and online connections and the use of these platforms to locate jihadist leaders and their followers.

Rehabilitation

This strategy uses moderate preachers to counsel terrorists and to instill in them a more balanced view of Islamic teachings. Singapore's counter-ideological program founded by Muslim scholars who seek to "correct" the thinking of its detainees is one such example (Ramakrishna, 2005). Established in 2003, the Religious Rehabilitation Group is an unpaid, all volunteer group of Islamic scholars who supplement their formal religious training with a year-long course in counseling.[14] Even before counseling sessions can begin, both male and female counselors study the "Jihad Manual" that prepares them to counter terrorists' ideological distortions. Typically one counselor works with a member of the Singaporean Internal Security Department and a government psychologist on a particular detainee. In 2005 counselors began working with detainees' families, especially the spouses, aided by the Interagency After-Care Group, which focused on the welfare of the detainees' families. The Interagency After-Care Group provides financial assistance, teaches wives skills and helps them find work, and ensures the continued education of the children by negotiating school fee waivers and providing them with pocket money. The Religious Rehabilitation Group also extends its influence into the wider Muslim community by giving talks, sponsoring fora, disseminating publications, and even hosting a website, the aim of which is to "immunize" the minds of Singaporean Muslims against violent radical Islamist ideologies. In addition, the Singapore government is attempting to forge closer ties between Muslims and non-Muslims through the

Community Engagement Program, Inter-Racial Confidence Circles in neighborhoods, workplaces and schools. Similar rehabilitation programs also have been introduced to other countries such as Indonesia, Saudi Arabia and Yemen.[15]

Summary

Table 1 lays out the two broad approaches to combating terrorism discussed above: Kinetic and Non-Kinetic. Two strategies fall within the kinetic approach (Targeting and Capacity-Building) and four fall within the non-kinetic approach (Institution Building, Psychological Operations, Information Operations and Rehabilitation). Within each generic approach, leadership can be either US or host-nation led.

Approach	**Kinetic**		**Non-kinetic**			
Leadership	U.S	Host Nation	U.S.		Host Nation	
Strategies	Targeting	Capacity Building	IB	PsyOp	IO	Rehab

Table 1: Combating Terrorism: Approaches and Strategies

Issues in the Use of SNA to Counter Terrorism

Having established our strategic framework, we now turn our attention to the specific role that social network analysis (SNA) can play in understanding terrorist networks. In our opinion while the use of SNA to analyze terrorist networks has been enlightening to date, it remains incomplete on at least three counts. First, there has been a lack of clarity and consistency as to what types of ties researchers have analyzed. In some instances researchers have analyzed kinship, friendship and acquaintance ties (e.g., Pedahzur & Perliger, 2006); in others they have analyzed kinship, friendship, acquaintance and operational ties (e.g., Sageman, 2004); in still others it is not altogether clear (e.g., Jordan, Mañas, & Horsburgh, 2008). To be sure, data collection is often driven by whatever network data are available, but rare has been the case when researchers have gathered and analyzed network data on a wide array of relations and been explicit about the types of ties analyzed and what constitutes a tie (for two notable exceptions, see Magouirk, Atran, & Sageman, 2008; Rodriguez, 2005). However, not only do we strongly believe that researchers need to be explicit about the data they collect and analyze (e.g., providing definitions of particular types of ties), they also need to collect network data on as many types of relations as possible. It is only by doing the latter that we can we begin to capture the complex nature of the networks we study (Breiger, 1975, cited in Azarian 2005; Simmel, [1908, 1922] 1955; White, 2008), for "it is a basic assumption of… the network approach that behavior cannot be explained in terms of any one single activity" (Breiger 1975, cited in Azarian, 2005).[16]

A second weakness in the extant literature is that the focus has been on individual level networks although there have been occasional forays into the subgroup and institutional levels (for a similar critique, see Asal & Rethemeyer, 2006). Pedahzur and Perliger (2006), for example, examine primarily individual level networks, but they do use k-core analysis to identify cohesive subgroups within the larger terrorist networks.[17] Similarly, Magouirk, Atran and Sageman (2008) devote most of their efforts to individual level networks, but they do use attribute data (e.g., role – suicide, bombing, planning) to identify subgroups within the larger network. As best we can tell, however, analysis at the sub-group level has been cursory at best and few researchers have engaged in a detailed examination of the institutional (i.e., organizational) level of dark networks (for an exception, see Asal & Rethemeyer, 2008). As social

movement scholars have repeatedly pointed out, however, insurgencies rely on the network of formal and informal organizations to help form and sustain the moral outrage that pushes people to join insurgencies, to help link people to insurgencies, and to help facilitate the mobilization and deployment of insurgent activities (Diani & McAdam, 2003; McAdam, 1999; Smith, 1991, 1996). Given the key role that these interorganizational networks play, it seems incumbent upon those of us who use SNA to combat terrorism that we devote some of our energies to analyzing and developing strategies for weakening the institutional networks of terrorist organizations.

Finally, in our opinion there seems to be far too much emphasis on using centrality and brokerage measures (or variations on them) to identify high-value targets within dark networks (Jordan, et al., 2008; Krebs, 2001; Pedahzur & Perliger, 2006; Sageman, 2004)—for a similar critique, see Tsvetovat and Carley (2005). As we noted earlier, identifying high-value targets is an important option to consider, but we want to encourage analysts to consider the wide variety of SNA metrics available, many of which we believe will prove useful in combating terrorist networks. This is not to say that we should abandon the use of centrality metrics. Indeed, we employ them extensively in our analysis below. However, we use them in conjunction with other algorithms (e.g., blockmodeling, centralization, density, QAP correlation) and for more than simply identifying high-value targets. What we are suggesting, in other words, is that analysts view centrality metrics as one set of SNA algorithms among many that can be used to help flesh out a range of strategic options. For example, at the individual level, centrality (e.g., degree, closeness, betweenness) and brokerage (e.g., structural holes, cutpoints, and Gould and Fernandez brokerage scores) algorithms can be used to identify key and peripheral players within the network, while blockmodel (e.g., structural and regular equivalence) and cohesion (e.g., cliques, components, k-cores) algorithms can be used to identify subgroups that could possibly be set at odds with one another. Similarly, centrality, brokerage, and (occasionally) blockmodel and cohesion routines can be used to distinguish between key and peripheral institutions and distinct subgroups at the institutional level. Analysts can also examine at the network's topographical characteristics (e.g., density, centralization) to get an overall sense of its overall dynamics (Everton, Forthcoming).

To briefly summarize our argument to this point, we believe that in order to effectively use SNA to combat terrorist networks, analysts need to collect multi-relational (i.e., multiplex) data, be explicit about the various types of ties they code and examine, analyze data at multiple levels of analysis (i.e., individual, subgroup, and organizational/institutional), and use the wide variety of SNA algorithms available to them. Most importantly, decisions surrounding data collection and analysis need to be informed by theory or some overarching conceptual framework. We will address each of these issues in their turn using data on Noordin Mohammad Top's terrorist network of South East Asia.

Noordin Top's Terrorist Network of South East Asia

The case study of Noordin Top's terrorist network of South East Asia lends itself to a demonstration of how to conduct a conceptually-driven, multi-relational, multi-layer, and multi-metric analysis of a terror network. Prior to his death in September of 2009, Noordin Mohammad Top was Indonesia's most wanted terrorist. He is believed to have been a key bomb maker and financier for Jemaah Islamiyah (JI) before leaving JI to set up his own, more violent, network. Long sought by Malaysian and Indonesian authorities, in 2006 he was also listed on the FBI's Seeking Information - War on Terrorism list (Wikipedia, 2010). Since 2001, the International Crisis Group (ICG) has assembled a series of reports on Indonesia that include details on Top's involvement in the October 2002 Bali bombing (Bali I), the August 2003 Marriot Bombing in Jakarta, Australian embassy bombing in Jakarta in September 2004, the second Bali bombing of October 2005 (Bali II), and the Jakarta bombings of the Marriott and the Ritz-Carlton in July 2009.[18] Since our purpose for this paper is methodological rather than historical, we only utilize the data from the 2006 ICG report entitled "Terrorism in Indonesia: Noordin's Networks" (2006) to illustrate how

data can be structured and analyzed to support the development of either kinetic or non-kinetic strategies to counter terrorism.

Data Structuring

The ICG 2006 report on Noordin contains rich one and two-mode network data on a variety of relations (e.g., friendship, kinship, internal communications) and affiliations (e.g., schools, religious, businesses and finance, functional location, operations, organizations, training events) – please see Appendix A for detailed description of the types of relations used in this analysis.[19] Some readers will rightly question whether we can infer a tie between two actors simply because they share an affiliation (e.g., attended the same school). In some cases it is clear-cut that we can. For instance, the number of individuals involved in the business and financial organizations were small, as were the teams that participated in the four operations included in this analysis and the individuals who participated in the various training events. Consequently, we believe that it is highly likely that ties did form between actors who jointly participated in these events and organizations. Inferring ties from the other affiliations (e.g., organizational, school, functional location) is less clear. In fact, if we were examining a "light" network (i.e., an overt and legal network) where joint affiliation in an organization and/or participation in the same event does not guarantee interaction between all actors, we would not make such an assumption. Here, however, we are dealing with a dark network where recruitment most likely occurred along ties of trust, where if two individuals who did not know one another prior to joining the network but shared a common friend, it is likely that a tie will form between them (Granovetter, 1973). We believe that in such an context, if two individuals attended the same school (not necessarily at the same time), were members of the same terrorist organization, provided functional support to Noordin's network in the same location, or attended the same mosque, there is a high probability that a tie formed between them. In fact, we believe that not inferring a tie in this context would lead us to underestimate the number and types of ties in the network under examination.

For demonstration purposes, we constructed two individual level one-mode networks: an operational network and a trust network.[20] Both are multi-relational (i.e., multiplex, stacked) networks as opposed to valued networks since the former lend themselves to visualizing the various relations separately or in combination with one another.[21] We also derived two one-mode institutional networks from the terrorist organizational and educational (i.e., school affiliation) networks. While our network visualizations use these multi-relational networks, we use dichotomized versions of the networks to calculate network metrics.[22] Table 2 summarizes key network statistics of the networks used in our analysis. As one can see all of these networks vary considerably in terms of their overall topography. Some are quite dense (e.g., the organizational network), while others are relatively centralized (internal communications). We will return to some of these metrics later in the paper.

	Density	Average Degree	Clustering Coefficient	Centralization
Operational Ties				
Communications	.055	4.30	.370	.412
Logistical Place	.017	1.29	.163	.154
Operations	.031	2.38	.248	.232
Financing	.006	.43	.072	.073
Organizational	.246	19.19	.765	.326
Training	.040	3.09	.382	.157
Aggregated	.307	23.97	.757	.448
Trust Ties				
Friendship	.029	2.23	.204	.129
Kinship	.004	.30	.000	.022
Religious	.004	.30	.074	.049
School	.055	4.30	.295	.233
Aggregated	.084	6.56	.356	.216
Institutional-Level				
Organizational	.165	2.14	.410	.526
School	.190	2.67	.562	.275

Table 2: Basic Metrics of Networks Used in Analysis

Data Analysis

Data structuring is an important first step in both the kinetic and the non-kinetic approaches to countering terrorism. A second, and just as important, step is to lay out a series of options one might want to explore before intervening into a particular network. Here, we have chosen to illustrate four such options (although clearly there are more), two that use a kinetic approach and two that use a non-kinetic approach: (1) A PsyOp strategy aimed at the individual level of the operational network; a (2) Targeting strategy aimed at the institutional level of the operational network; a (3) Targeting strategy aimed at the individual level of the trust network; and an (4) Institution-Building strategy aimed institutional level of the trust network.

PsyOp Strategy (Non-Kinetic): Operational Network, Individual Level

Noordin's operational network is presented in Figures 1a through 1d where node size indicates degree, closeness, betweenness and eigenvector centrality respectively. One can see that is fairly dense (.307) and relatively centralized (.448) – see Table 2. At first glance the results from the calculation of common centrality measures identify several key actors who could serve as kinetic action targets (see Table 3). Eight individuals (highlighted in bold print) rank in the top ten of all four measures, suggesting that no

matter how we slice the data, these individuals are high value targets, and Noordin's presence at the top of the list is no surprise since it is his network after all.

Once we move past him, however, the amount of variation in the centrality scores is minimal. (This is more obvious in Figures 1a through 1d than in Table 3—a fact that points to the importance of why metrics should almost always be used in conjunction with network visualizations). This lack of variation should make us cautious (at least in this case) of using centrality metrics to identify key players for capture or elimination. In most counterterrorism operations resources and intelligence are limited, which makes targeting more than a handful of individuals extremely difficult. Moreover, as other have noted strategies that focus on the isolation of highly central individuals are often ineffective in the long run because networks tend to heal themselves relatively quickly (Pedahzur & Perliger, 2006; Tsvetovat & Carley, 2005).

Degree	Closeness	Betweenness	Eigenvector
Noordin Top (74.36)	**Noordin Top** (.802)	**Noordin Top** (14.88)	**Noordin Top** (25.97)
Azhari Husin (58.97)	**Azhari Husin** (.713)	**Ahmad Rofiq Ridho** (5.70)	**Azhari Husin** (25.89)
Chandra (58.97)	**Chandra** (.713)	**Chandra** (3.68)	**Chandra** (24.63)
Abdullah Sungkar (57.69)	**Abdullah Sungkar** (.706)	**Abdullah Sungkar** (3.43)	Ubeid (24.39)
Abu Bakar Ba'asyir (56.41)	**Abu Bakar Ba'asyir** (.700)	Hari Kuncoro (3.12)	**Imam Samudra** (24.37)
Ahmad Rofiq Ridho (56.41)	**Ahmad Rofiq Ridho** (.700)	**Azhari Husin** (3.00)	**Abdullah Sungkar** (24.36)
Imam Samudra (55.13)	**Imam Samudra** (.694)	**Abu Bakar Ba'asyir** (2.86)	**Abu Bakar Ba'asyir** (24.27)
Ubeid (55.13)	Ubeid (.694)	Iwan Dharmawan (2.73)	**Usman bin Sef** (24.25)
Usman bin Sef (55.13)	**Usman bin Sef** (.694)	**Imam Samudra** (2.42)	**Ahmad Rofiq Ridho** (24.06)
Hari Kuncoro (53.85)	Hari Kuncoro (.688)	**Usman bin Sef** (2.41)	Umar Wayan (24.01)

Table 3: Top 10 Ranked Individuals of Operational Network by Normalized Centrality Scores (scores in parentheses)

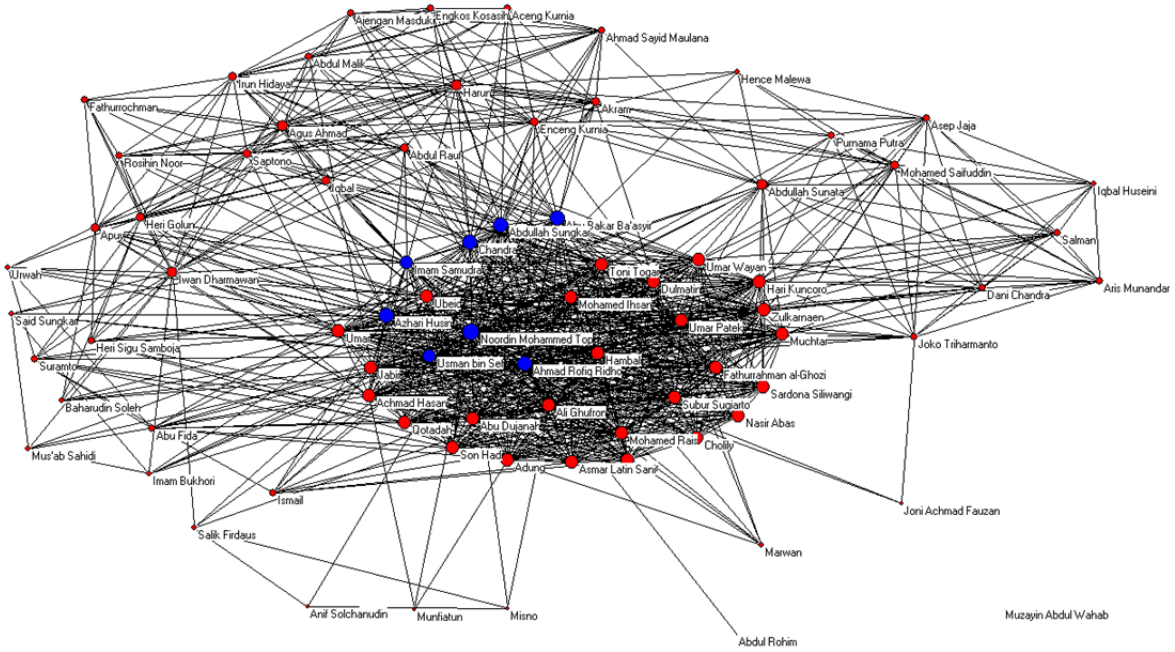

Figure 1a: Operational Network (Degree Centrality)

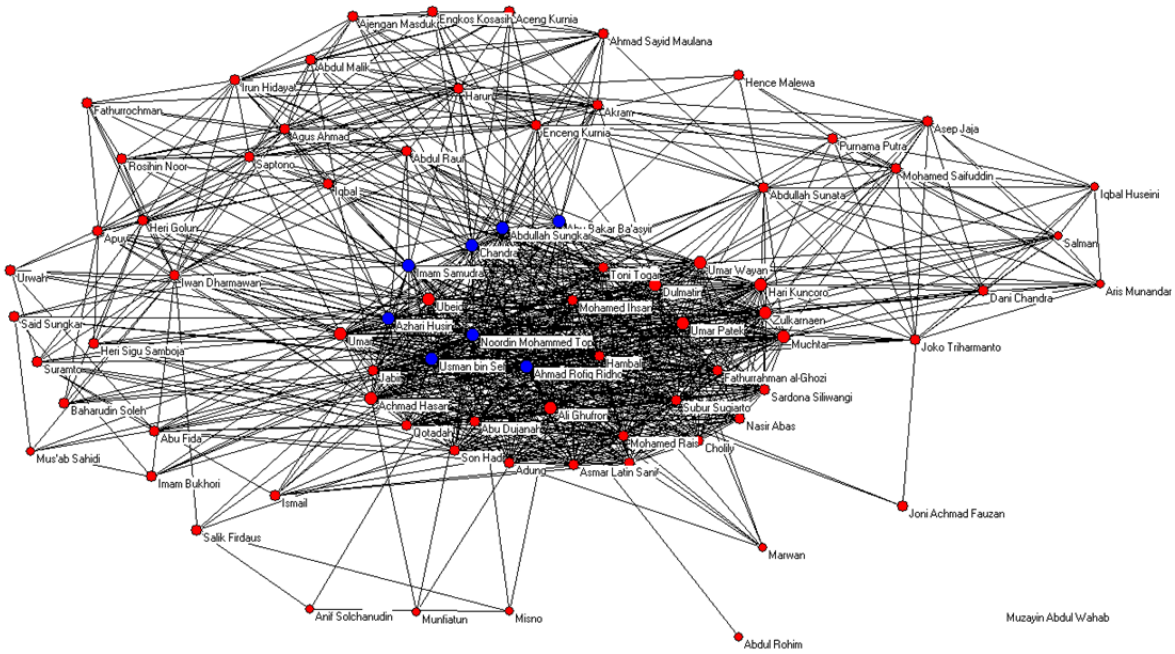

Figure 1b: Operational Network (Closeness Centrality)

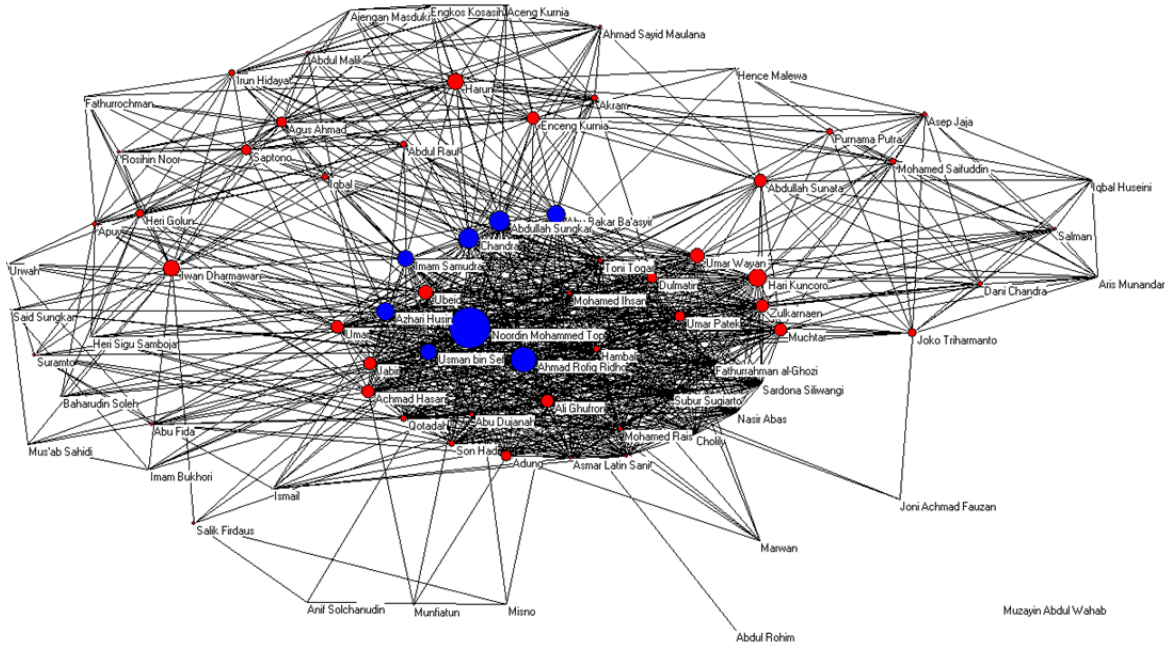

Figure 1c: Operational Network (Betweenness Centrality)

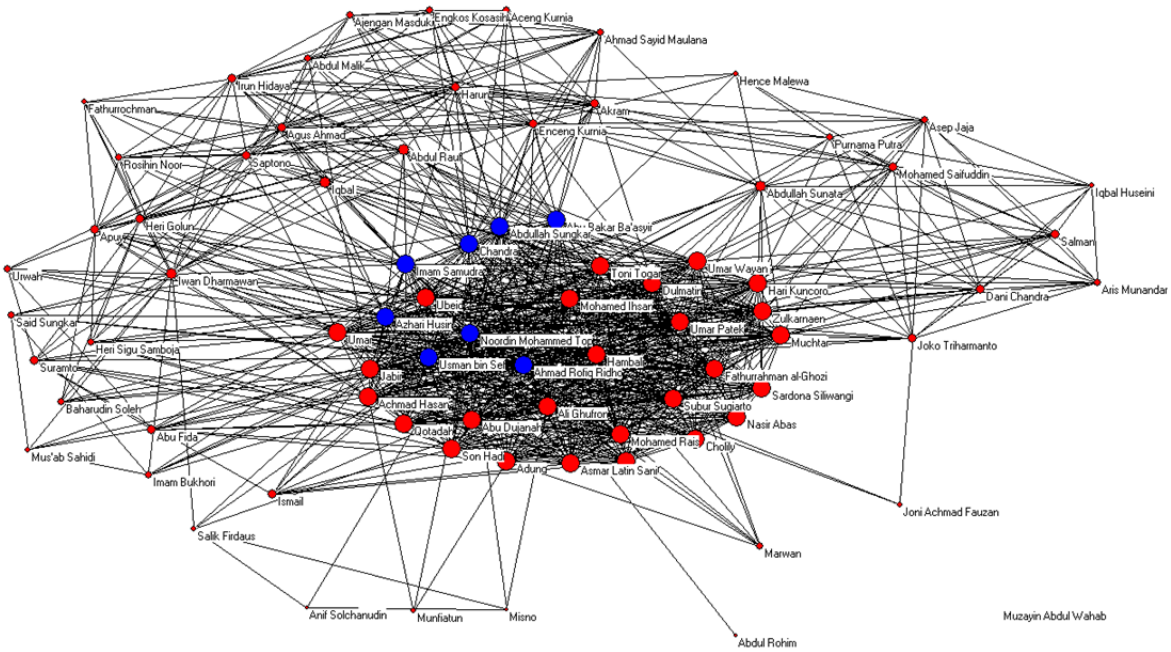

Figure 1d: Operational Network (Eigenvector Centrality)

An alternative, non-kinetic approach would be to use these highly central actors as key nodes in a deception campaign where information is inserted into a network at those points "where the messages and observables will resonate the greatest" (Anonymous, 2009:8-9). Such an approach was recently implemented with success in northern Iraq. Intelligence officers identified actors in an insurgent network who scored high in terms of betweenness centrality as information insertion points.[23] The effort was so successful in rolling up the insurgency, by the end of this group's tour in Iraq, this method of using SNA for deception operations had become standard operating procedure (Anonymous, 2009:9).

Targeting Strategy (Kinetic): Operational Network, Institutional Level

What is striking about Noordin's operational network is that there appears to be a core group of individuals lying at its center. The color of the nodes in Figure 2 captures this core (blue)—periphery (red) structure.[24] The figure also separately highlights each type of relation (organizational, business/finance, terrorist operations, logistical place, training and internal communications). As should be clear from the figure, while it appears that there are a handful of overlapping ties, organizational ties appear to form the basis of Noordin's operational network.[25]

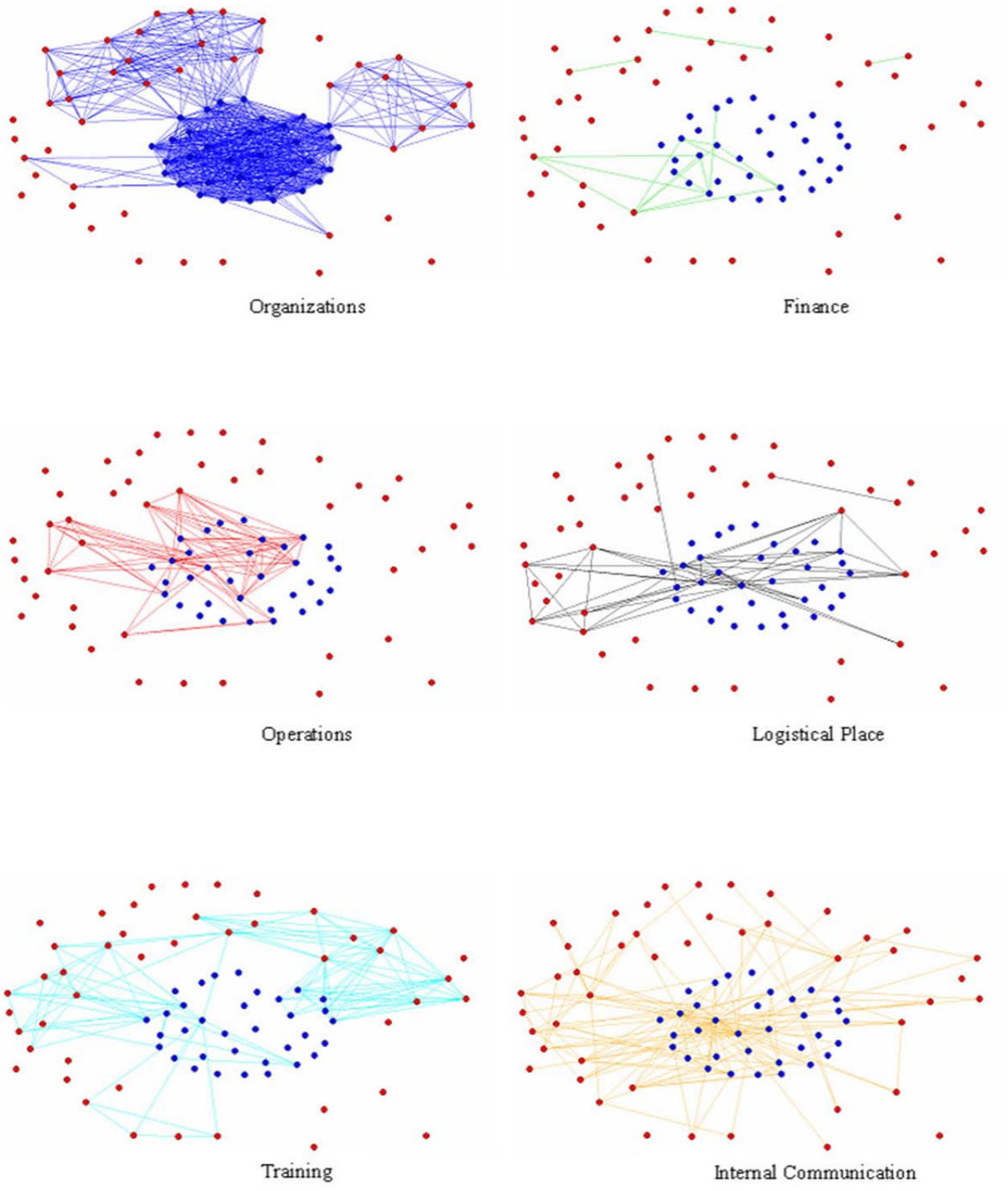

Figure 2: Noordin Top Operational Network

This suggests that if analysts are interested in helping Indonesia craft a kinetic strategy to disrupt or destabilize Noordin's network, they may want to redirect their focus from the individual to the institutional level. Figure 3 visually does just this where the mapped network is not the individual level operational network but instead the operational aspect of the institutional level network, for as we just saw, organizational ties appear to play a central role in Noordin's operations. In Figure 3 a tie between two terrorist organizations indicates that they share at least one common member, while the width of the ties varies according to the number of ties between organizations.[26] Jemaah Islamiyah (JI) clearly lies at the center of this network, which suggests that Indonesia may want to pursue strategies that seek to limit JI's ability to function by shutting down its publishing houses (International Crisis Group, 2008), eliminating other sources of financing (see below), and so on. Of the other organizations that appear to be central to Noordin's operations, Mantiqi I, JI's regional affiliate located in mainland Malaysia and Singapore, strikes us as the best target given its fundraising focus. A successful blow to its fundraising apparatus could leave the larger JI movement unable to mobilize enough resources to be much of a threat, for as social movement scholars have taught us, it is difficult if not impossible for an insurgency to mobilize without adequate resources (McAdam, 1982; McCarthy & Zald, 1977; Wiktorowicz, 2004).

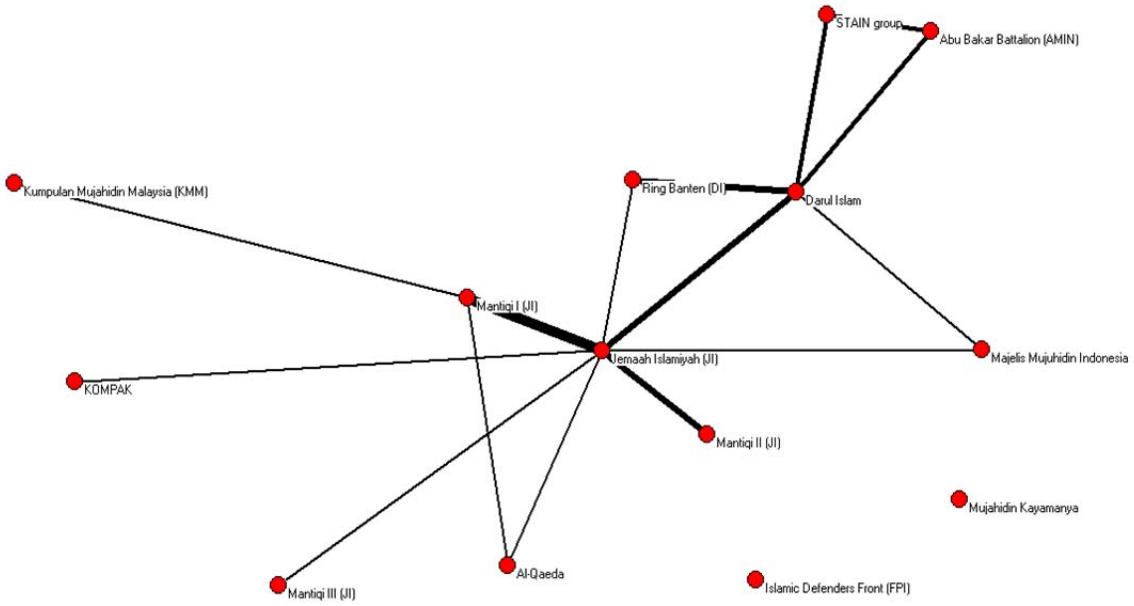

Figure 3: Terrorist Organizational Network (width of line reflects number of ties between organizations)

Targeting Strategy (Kinetic): Trust Network, Individual Level

Figure 4 presents a visual map of Noordin's trust network, which as noted earlier consists of the friendship, kinship, religious and school network (see Appendix A for detailed description of these types of ties). The structure of this network differs from the operational network. It is less dense (.0841) and less centralized (.216)—see Table 2—but like the former it has a distinct core (blue) – periphery (red) structure.[27] The core is so dense (1.00) that it is unlikely that any strategy would be able to pry these core members away from the network through an amnesty and/or reconciliation program, so we may want to target key actors for capture or elimination. Table 4 presents the top-ranked individuals in the trust network according to degree, closeness, betweenness and eigenvector centrality. Surprisingly, Noordin is

not as central in this network as he is in the operational one. He appears in the top ten only in terms of closeness and betweenness. What is interesting is that unlike the operational network where we identified eight individuals who scored high on all four measures of centrality, here we find only three, who are circled in Figure 4 (blue nodes) along with Noordin (red node). As we can see these actors sit on the edge of the core, essentially connecting the core with the other members of the network. This suggests that capturing or eliminating these individuals could help isolate the core and limit its effectiveness.

Before pursuing such a strategy, however, we may want to consider the second-order effects of targeting a key member of a trust network. As we noted earlier evidence suggests that dark networks heal rather quickly, often rendering targeting approaches relatively ineffective. Targeting key members could also strengthen the resolve of those still alive to avenge their comrade's death.[28] Thus, analysts may want consider a non-kinetic strategy for disrupting the network, the approach to which we turn next.

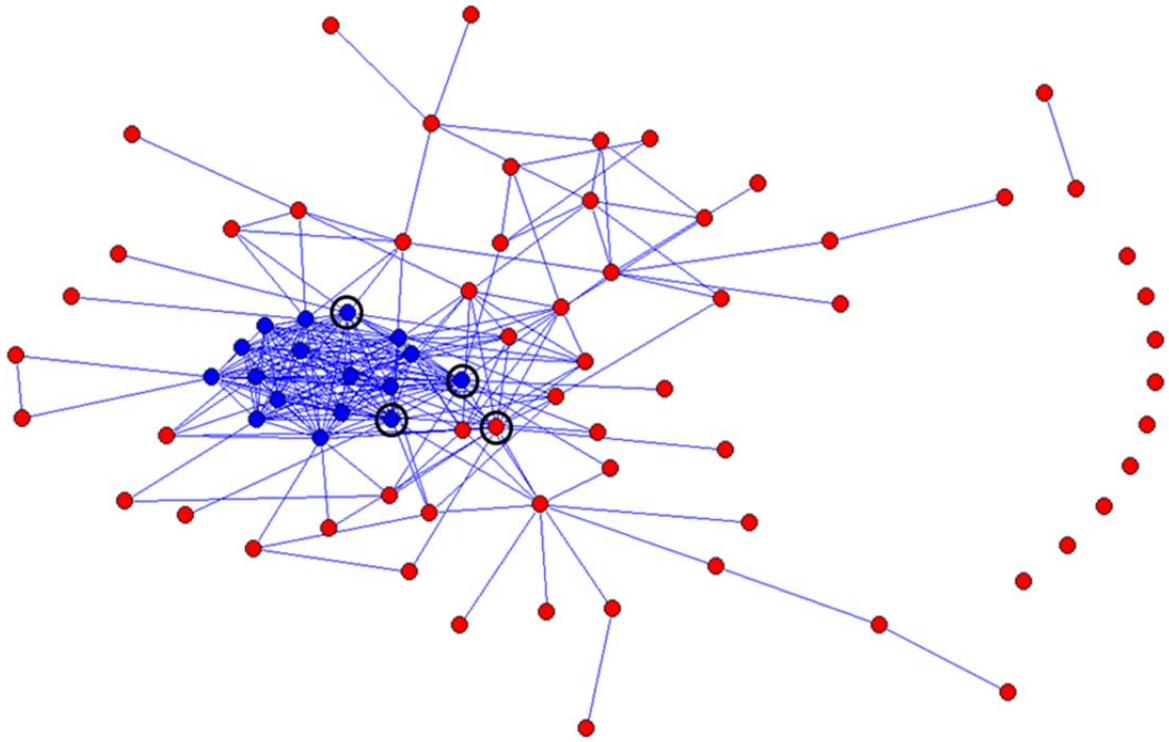

Figure 4: Trust Network

Degree	Closeness	Betweenness	Eigenvector
Ahmad Rofiq Ridho (29.49)	**Ahmad Rofiq Ridho** (53.60)	**Ahmad Rofiq Ridho** (19.41)	Mohamed Rais (35.64)
Adung (28.21)	**Ubeid** (50.76)	Iwan Dharmawan (17.25)	Tohir (35.64)
Jabir (28.21)	Adung (48.91)	Abdullah Sunata (10.87)	Jabir (34.70)
Mohamed Rais (28.21)	Mohamed Rais (48.55)	**Ubeid** (8.46)	Adung (34.30)
Tohir (28.21)	Tohir (48.55)	Noordin Top (8.13)	Asmar Latin Sani (34.22)
Son Hadi (26.92)	**Son Hadi** (47.86)	Adung (7.15)	**Son Hadi** (33.83)
Ubeid (26.92)	Jabir (47.52)	Usman bin Sef (6.27)	**Ubeid** (33.54)
Asmar Latin Sani (24.36)	Asmar Latin Sani (46.53)	**Son Hadi** (4.59)	**Ahmad Rofiq Ridho** (33.42)
Suramto (24.36)	Suramto (46.53)	Akram (4.58)	Suramto (33.25)
Zulkarnaen (23.08)	Zulkarnaen (45.58)	Zulkarnaen (4.33)	Fathurrahman al-Ghozi (32.50)
	Noordin Top (45.58)	Agus Ahmad (4.33)	Toni Togar (32.50)

Table 4: Top 10 Ranked Individuals of Trust Network by Normalized Centrality Scores (scores in parentheses)

Institution Building Strategy (Non-kinetic): Trust Network, Institutional Level

Just as Noordin's operational network was constituted primarily by a single set of relations, so too is Noordin's trust network. Figure 5 presents the network, broken down by school, religious, friendship and kinship ties. As one can see, while a number of ties do appear to overlap,[29] school ties appear to form the basis of the trust network, with the other networks, in particular the friendship network, reaching out and pulling the other actors in.[30]

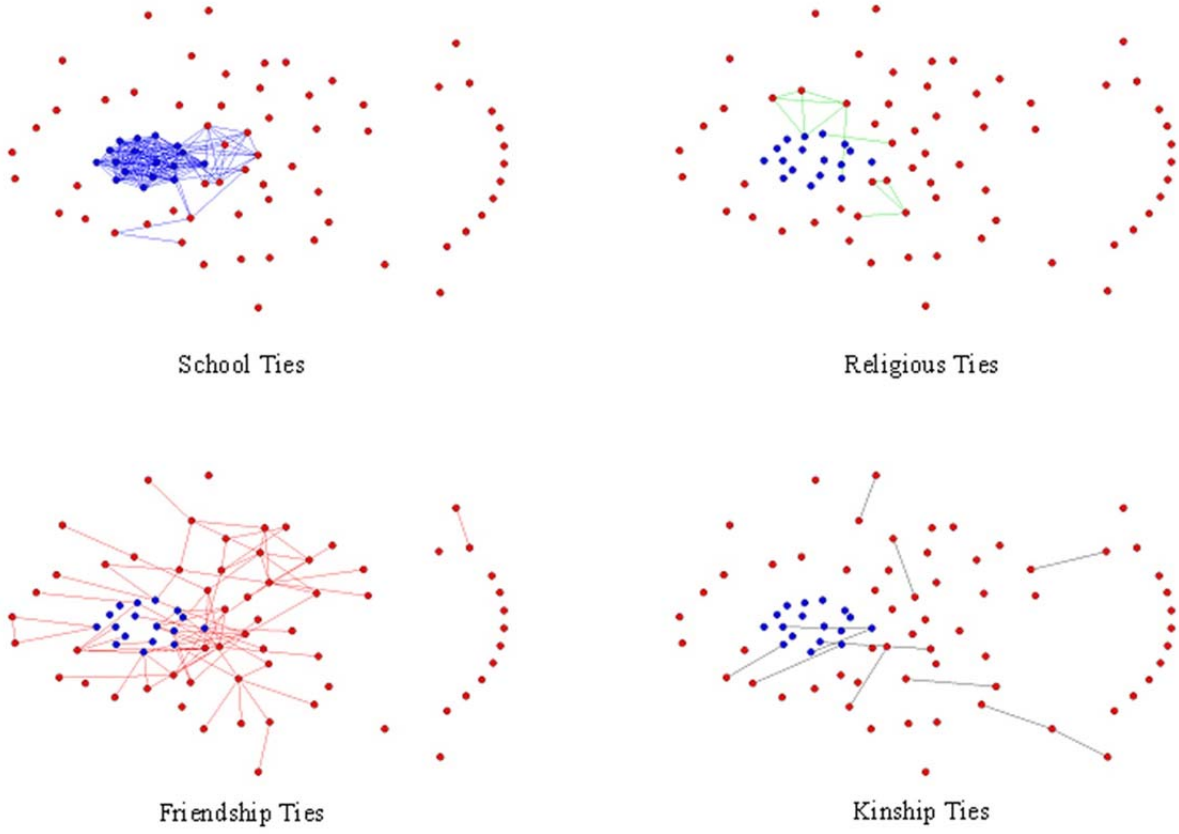

Figure 5: Trust Network

Figure 5: Trust Network

The central role that school ties play in the trust network indicate that a disruption strategy aimed at the institutional school network may prove fruitful. As Table 5 and Figures 6a-6d indicate, there are three peasentrens (i.e., Islamic boarding schools) that play key roles within the Noordin Top terrorist network: Pondok Ngruki, Universitas an-Nur and Luqmanul Hakeim. A kinetic approach would probably attempt to close these schools (indeed, that is what the Indonesian authorities did with the Luqmanul Hakeim school) so that they can no longer serve as ideological training grounds for Noordin, JI or any other Islamic insurgent group of which Indonesia has plenty (Banlaoi, 2009). A non-kinetic approach, on the other hand, might seek to use locals to infiltrate these schools to improve intelligence gathering although this is often easier said than done. Another non-kinetic option would be to build alternative schools near-by these three schools, ones that promote moderate forms of Islam and instruct students in subjects other than the memorization of the Qur'an (e.g., reading, writing and arithmetic). This latter example would be a variation on the Institution Building strategy discussed earlier, and one that we like to call the "Three Cups of Tea" approach to combating terrorism (Mortenson & Bryan, 2009; Mortenson & Relin, 2006).[31] This is clearly a long-term strategy, one that aims not so much at disrupting the current configuration of Noordin's network but rather one that aims to deprive Noordin (or his successors) of a key resource (McAdam, 1982; McCarthy & Zald, 1977; Wiktorowicz, 2004).

Degree	Closeness	Betweenness	Eigenvector
Pondok Ngruki (42.86)	**Pondok Ngruki** (63.16)	**Pondok Ngruki** (43.96)	**Universitas an-Nur** (69.11)
Universitas an-Nur (42.86)	**Universitas an-Nur** (57.14)	**Universitas an-Nur** (30.77)	**Pondok Ngruki** (68.98)
Luqmanul Hakeim (28.57)	**Luqmanul Hakeim** (50.00)	**Luqmanul Hakeim** (29.67)	al-Husein (50.22)
Adelaide University (21.43)	al-Husein (48.00)	al-Muttaqien (12.09)	Indramayu (50.22)
al-Husein (21.43)	Indramayu (48.00)		Darusysyahada (36.83)
al-Muttaqien (21.43)	Darusysyahada (46.15)		**Luqmanul Hakeim** (33.89)
Indramayu (21.43)			
Reading University (21.43)			
Univ. of Technology, Malaysia (21.43)			

Table 5: Top Ranked Schools by Normalized Centrality Scores (scores are in parentheses)

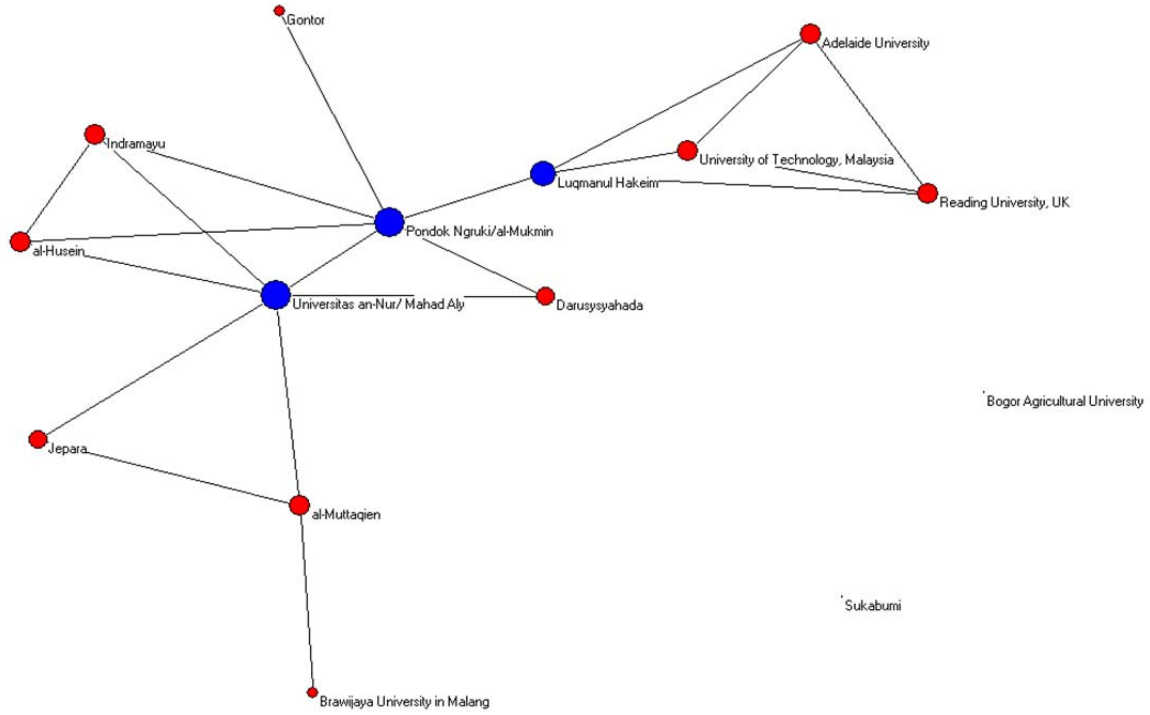

Figure 6a: School Network (Degree Centrality)

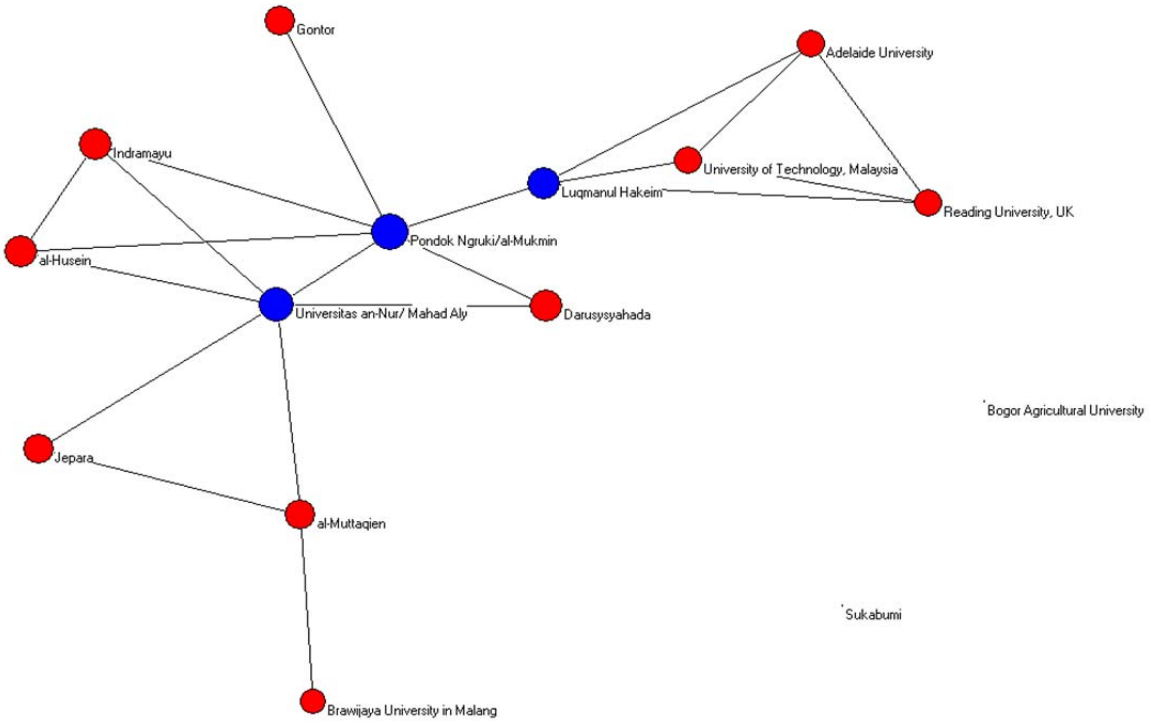

Figure 6b: School Network (Closeness Centrality)

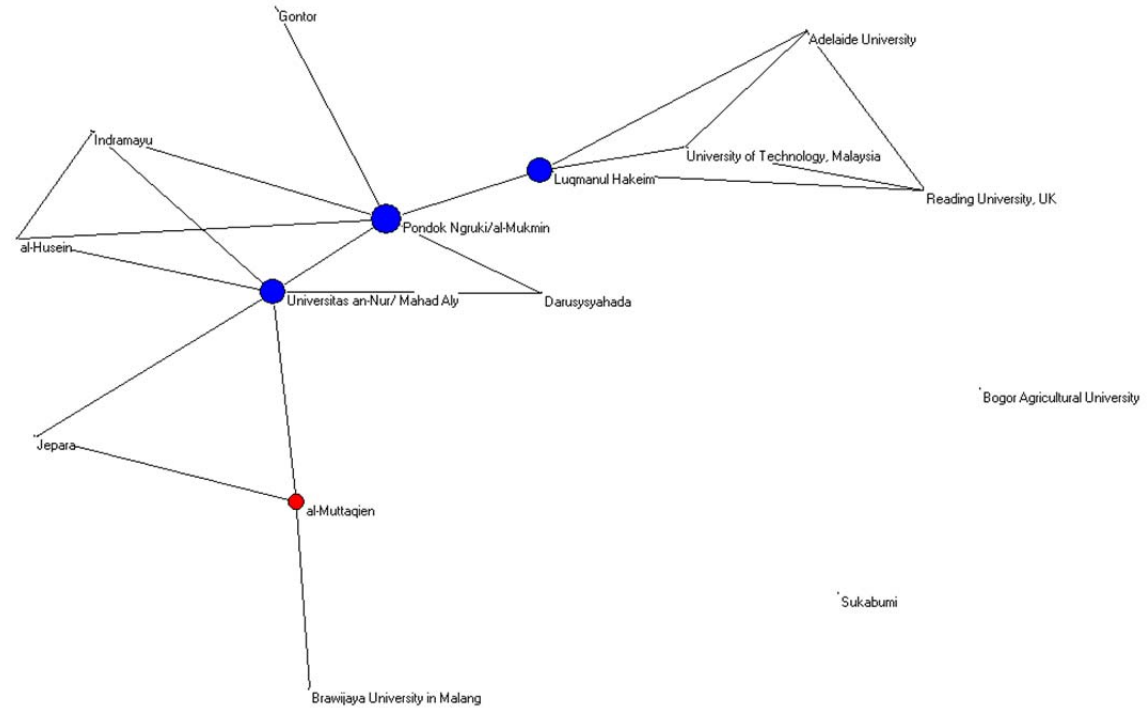

Figure 6c: School Network (Betweenness Centrality)

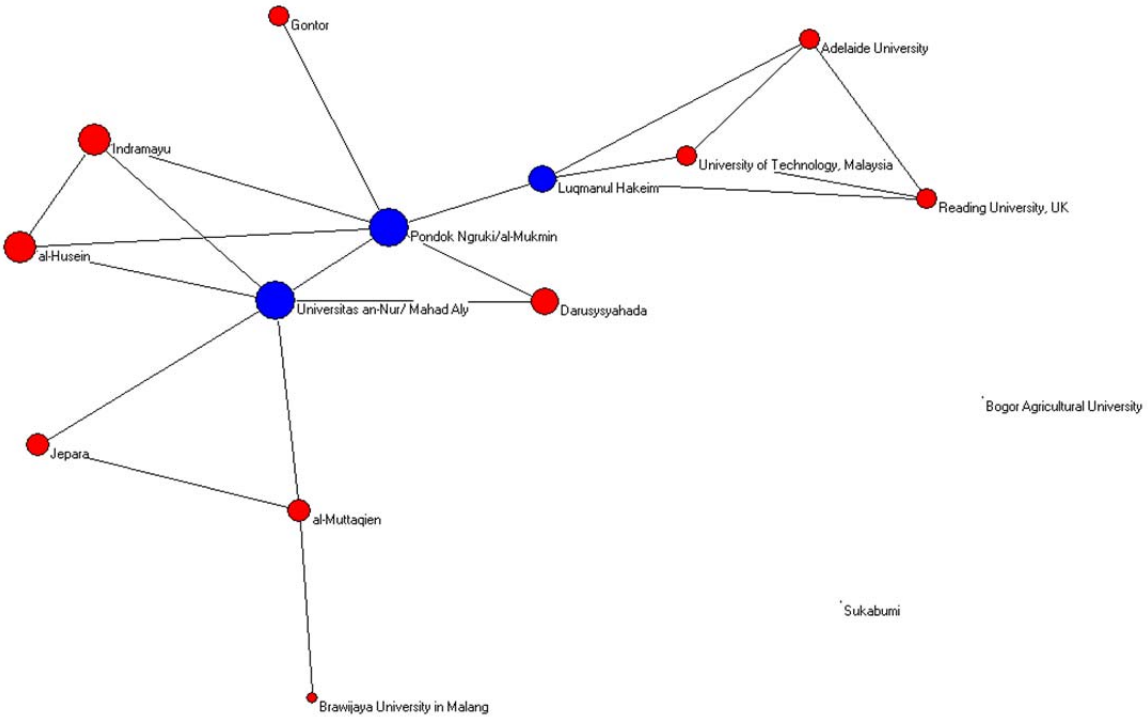

Figure 6d: School Network (Eigenvector Centrality)

Conclusion

Combating terrorism is a complex endeavor. Unfortunately, in our review of the literature we have found no systematic framework for identifying alternative strategies to combat terrorism, nor have we found any theoretical or empirical studies to support or justify the pursuit of one strategy over another. What counter-insurgency and counter-terrorism strategies should we pursue and under what conditions? And what trade-offs should we make and what are the likely consequences of our strategic choices? Currently, we have few empirically- or theoretically-grounded answers in response to these questions.

To begin to address this void, our paper presents a typology of kinetic and non-kinetic approaches to combating dark networks. From the kinetic approach we derive two strategies*: Targeting* and *Capacity-Building*. From the non-kinetic approach, we derive four: *Institution-building*, *Psychological Operations*, *Information Operations, and Rehabilitation*. Although these strategies are conceptually distinct, we do not assume that they are mutually exclusive or constitute a comprehensive list. It is possible, for example, that strategies can be sequenced or combined in some manner in order to achieve greater effect. Future theory development and research will be required to refine our typology and make finer-grained distinctions. We offer this paper as a first step in this effort.

We also have identified three major weaknesses in the current research on dark networks. First, there has been a lack of clarity and consistency as to what types of ties are under study. Not only do researchers need to be clear on which ties they are collecting and analyzing, they should base their analyses on multi-relational data to capture the complexity of dark networks. As we illustrated with the Noordin Top data set, dark networks consist of numerous relations—both trust and operational—some that lend themselves to developing kinetic strategies and others that lend themselves to non-kinetic ones. Thus, we need to expand our data collection efforts to include a range of relations among network members and base our choice of ties on the conceptual and theoretical frameworks that inform our studies.

A second weakness we highlighted is that most SNA analyses of dark networks have focused almost exclusively on individual level networks with little or no attention paid to the subgroup and institutional (i.e., organizational) levels of dark networks. Given the important role that inter-organizational networks almost always play in the recruitment and mobilization of insurgencies, this strikes us as an area for increased research activity. As we demonstrated in our analysis, certain institutions appear to play a central role in the functioning of Noordin Top's terrorist network. We also showed how we can use both kinetic and non-kinetic strategies for rendering such institutions less effective.

Finally, intelligence analysts, field operatives, and researchers using SNA to disrupt dark networks appear to be putting the cart before the horse. They tend to begin (and end) their analysis with centrality and/or brokerage metrics to identify a dark network's central players, which often leads to the pursuit (i.e., the targeting) of those players. We take issue with this choice on two counts. First, as we have demonstrated, other social network analysis metrics can be useful in identifying high-value actors within networks. While we used a variety of centrality metrics in this paper, we used them in conjunction with blockmodeling, centralization, density and correlation algorithms to identify other key features of the network (e.g., core and periphery structures) in order to inform our analyses of the operational and trust networks. Moreover, we used these centrality metrics not simply to identify high value targets but rather in the service of both kinetic and non-kinetic strategies. This leads us to our second and, from our perspective, far more important point: namely, that the identification of key players depends on the strategy one pursues, not on the metrics one chooses. For example, key players in a rehabilitation strategy would likely be members at the network's periphery rather than at its core (since peripheral members are more likely to defect – see Popielarz & McPherson, 1995; Stark & Bainbridge, 1980), suggesting that when it comes to identifying detainees for its counter-ideological program, Singapore's Religious Rehabilitation

Group (see earlier discussion above) may want to identify actors who score low in terms of network centrality.

All of this is not to say that the ways that researchers who have used SNA to date have been invaluable. Nothing could be further from the truth. Indeed, much of what we illustrate in this paper builds upon their efforts. However, we do recommend that analysts and strategists embed their use of social network analysis within a larger strategic and/or theoretical framework. Most importantly, we believe they would benefit in using SNA to help them flesh out strategic options as we have demonstrated in this paper. Although understanding which strategic option to pursue and under what conditions remains more of an art than a science, we believe SNA has an important and growing role to play in the next generation of counter-terrorism efforts.

Appendix A

The Noordin Top Terrorist Trust Network data are drawn from the International Crisis Group's (2006) report on the terrorist networks of Noordin Mohammed Top, who is believed to be responsible for the 2003 JW Marriott Hotel and 2004 Australian Embassy bombings in Jakarta, the 2005 Bali bombing and the 2009 JW Marriott and Ritz Carlton bombings in Jakarta. The initial data were collected and coded by students as part of the "Tracking and Disrupting Dark Networks" course offered at the Naval Postgraduate School in Monterey, California, under the supervision of Dr. Nancy Roberts. Portions of the data have been updated by students in subsequent iterations of the course (through the spring of 2009) as well as from other articles and reports by Dr. Sean Everton. One and two-mode network data were collected on a variety of relations (e.g., friendship, kinship, internal communications) and affiliations (e.g., schools, religious, businesses, training events, operations).

Operational Network

- **Internal communications:** Defined as ties based on the relaying of messages between individuals and/or groups inside the network through some sort of medium.
- **Logistical place:** Defined as key places where logistical activity—providing materials, weapons, transportation and safehouses—occurred
- **Operations:** Includes terrorists who were directly involved with the Australian Embassy bombing, the Bali I Bombing, the Bali II bombing and/or the Marriott Hotel bombing, either at the scene (e.g., suicide bombers, commanders) or as a direct support to those at the scene (e.g., driver or lookout). It does not include ties formed through communications, logistics, or organizations related to the operations
- **Terrorist financing:** Defined as the for-profit and not-for-profit businesses and foundations that employ members of the network.
- **Terrorist organizational membership:** Defined as an administrative and functional system, whose primary common goal is the operational conduct of terrorist/insurgent activities, consisting of willingly affiliated claimant members. Factions, affiliates and offshoots are considered separate from their parent organization.
- **Training:** Defined as participation in any specifically designated activity that teaches the knowledge, skills, and competencies of terrorism. It does not include participation in a terrorist sponsored act or mujahedeen activity in places such as Afghanistan, Bosnia, Chechnya or Iraq unless the individuals' presence was to participate in a specifically designated training camp or base in one of these areas.

Trust Network

- **Friendship:** Defined as close attachments through affection or esteem between two people. Friendship ties do not include ties based on meetings and/ or school ties.
- **Kinship:** Defined as a family connection based on marriage. It includes current marriages and past marriages due to divorces and/or deaths.
- **Religious affiliation:** Defined as association with a mosque. It does not include Islamic schools—see next category—even though such schools have mosques.
- **School affiliation:** Educational relations are defined as schools where individuals received formal education. This includes both religious and secular institutions.

[1] Gang and criminal networks also are examples of dark networks (Baker & Faulkner, 1993; Sparrow, 1991), but our focus in this article is on terror and insurgency networks.

[2] http://www.nctc.gov/docs/Tide_Fact_Sheet.pdf [accessed January 5, 2011].

[3] http://ai.arizona.edu/research/terror/ [accessed January 5, 2011].

[4] Certainly there are critiques of counter-terrorism strategies (see e.g., Ettlinger & Bosco, 2004) and alternative strategies are proposed, e.g. non-military engagement with terrorism, but our search revealed no comparative research on counter-terrorism strategies.

[5] http://en.wikipedia.org/wiki/High_Value_Target [accessed January 5, 2011].

[6]There is no agreement in the literature on how to describe the alternative approaches to countering terrorism. Some authors use different characterizations e.g. direct and indirect strategies (Arreguin-Toft, 2001, 2005; Fridovich & Krawchuk, 2007; Krawchuk, ND). Our preference is to focus on the behavior of the combatants and the level of the coercion involved in their strategies and hence we have chosen to use the terms "kinetic" and "non-kinetic."

[7] The Non-Kinetic Approach is complex with different meanings and interpretations. See Brimley and Singh (2008) for a good overview of its various expressions.

8 The U.S. military has recently introduced the topic of social network analysis into its doctrine. See Appendix B of the *COIN Manual* (FM3-24) (U.S. Army, 2007). Our intent is to go beyond this descriptive effort to illustrate how SNA can be used to generate alternative strategies to counter terror and insurgencies.

[9] http://webcache.googleusercontent.com/search?q=cache:3EFgbX_1kPoJ:www.special-operations-technology.com/sotech-home/56-sotech-2008-volume-6-issue-4/423-qaa-admiral-eric-t-olson.html+%E2%80%9Curgent+and+necessary,%E2%80%9D+it+is+his+belief+that+it+is+%E2%80%9Cnot+decisive.+It+is+a+holding+action+that+buys+time+for+the+indirect+approach+to+have+its+decisive+effect.%E2%80%9D&cd=1&hl=en&ct=clnk&gl=us [accessed January 5, 2011]. Admiral Olson's use of the terms "direct" and "indirect" in this quote is another example of the variation in terms used to describe alternative counter-terrorism strategies.

[10] See Krawchuk (ND) and Fridovich and Krawchuk (2007) as examples.

[11] Note the use of the terms "direct" and "indirect" instead of "kinetic" and "non-kinetic."

[12] http://www.jihadwatch.org/dhimmiwatch/archives/019119.php [accessed January 5, 2011].

[13] In contrast to military doctrine (U.S. Director of Operations, 2006), we separate Psychological Operations and Deception from Information Operations. Information Operations puts a strong emphasis on technology-centric interventions that involve computer and other sophisticated electronic systems. Psychological Operations, in contrast, puts a strong emphasis on human factors. For that reason, we treat Psychological Operations as a separate strategy in combating terrorism rather than consider it as a subset of Information Operations.

[14] See the Religious Rehabilitation Group website at http://www.rrg.sg/main.asp [accessed January 5, 2011].

[15] For a review of Saudi Arabia's program, see Boucek (2008a, 2008b). The Report by Fink and Hearne (2008) on deradicalization and disengagement from violent extremism provides a general overview of topic. See also Horgan (2009) and Jones and Libicki (2008).

[16] For an excellent example of this see Il-Chul Moon's (2008) unpublished dissertation.

[17] They also use clique analysis, but not to identify cohesive subgroups but rather to get a sense of the network's overall structure.

[18] For a listing of these reports see http://www.crisisgroup.org/en/regions/asia/south-east-asia/indonesia.aspx [accessed January 5, 2011].

[19] The data were initially collected and coded by students as part of the "Tracking and Disrupting Dark Networks" course offered at the Naval Postgraduate School in Monterey, California, under the supervision of Nancy Roberts. Portions of the data have been updated by students from subsequent iterations of the course (under the supervision of Sean Everton) and by Sean Everton using additional articles and reports.

[20] We are using the two categories (operational and trust) for illustrative purposes as one way to think about these networks from a strategic perspective. Other subgroups could be used in the analysis of terror networks. For this paper we are treating all actors as alive and active although some have been captured and killed.

[21] Of course, we first derived one-mode networks from the affiliation networks before aggregating the networks together.

[22] Except where noted, we used Pajek (Batagelj & Mrvar, 2010) for our network visualizations and UCINET 6.0 (Borgatti et al. 2002) for calculating SNA metrics. We use dichotomized networks to calculate degree and eigenvector centrality measures because, here, we are interested in the count of the number of ties and not their weight (or strength). That said, we can envision instances where taking into account the weight or strength of ties is a better indicator of degree and eigenvector centrality than a dichotomized graph (e.g., when the strength of actors' ties is a predictor of an independently measured outcome such as influence, status, etc.).

[23] Another algorithm that may have proven useful is Borgatti's (2006) key player algorithm for identifying optimal sets of nodes to influence.

[24] We formally identified this core-periphery structure by estimating a two-block structural equivalence model using the optimization algorithm (error score = 772) implemented in Pajek (Batagelj & Mrvar, 2010; de Nooy, Mrvar, & Batagelj, 2005; Doreian, Batagelj, & Ferligoj, 2005). We chose to use a blockmodel approach here instead of the core-periphery algorithm available in UCINET to identify the core-periphery structure because visual inspection of the two resulting partitions indicated that the former approach provided a better visual fit of the data better than the latter. That said, the results were virtually identical and our conclusions would remain the same regardless of which partition algorithm we chose. The alternative results are available upon request.

[25] The highest level of correlation among the six networks is between the operational and internal communication networks: .186. The internal communication network overlaps somewhat with the business and finance network (.155), and the organizational network overlaps to a certain degree with the operational network (.142) and the internal communication network (.145).

[26] We have chosen not to vary node size degree, closeness, betweenness and eigenvector centrality since JI is clearly a cutpoint and will be most central in all cases. Thanks to *JoSS* editor James Moody for suggesting this.

[27]Using an optimization algorithm to estimate a two-block structural equivalence models for the trust network (Batagelj & Mrvar, 2010; de Nooy, et al., 2005; Doreian, et al., 2005) yielded an error score of 246. Here again we chose to use a blockmodel approach here instead of the core-periphery algorithm available in UCINET to identify the core-periphery structure because visual inspection of the two resulting partitions indicated that the former approach provided a better visual fit of the data better than the latter. The alternative results are available upon request.

[28] We thank *JoSS* editor James Moody for pointing this out to us.

[29] The highest level of correlation among the four networks exists between the friendship and school networks: .140. It is the only correlation coefficient that is statistically significant as well.

[30] It is possible that the lack of ties outside of the core could be the result of data collection procedures, but the two types of tie that are sparse (i.e., kinship, religious) are probably a reasonably accurate reflection of how this network is constituted. Noordin does appear to have looked more to friendship ties than kinship ties and recruited more heavily from JI schools than local mosques. He was a member of JI and taught at one or more of the JI schools.

[31] *Three Cups of Tea* (Mortenson & Relin, 2006) tells the true story of mountain climber Greg Mortenson who, after helping with the 75-hour rescue of another climber on K2, the world's second highest mountain, left him weak and disoriented, stumbled into a Pakistan village (Korphe) after taking a wrong turn on his descent. After being nursed back to health by the village, he vowed to return to the village and build them a school. It took him over two years to raise the funds and build the school, but in 1996, the Korphe School was completed. Since then, the institute (Central Asia Institute) he co-founded with Silicon Valley entrepreneur Dr. Jean Hoerni (see http://en.wikipedia.org/wiki/Jean_Hoerni [accessed January 5, 2011]) has built almost 80 schools in Pakistan and Afghanistan. Interestingly, while the subtitle of the paperback version of the book reads, *One Man's Mission to Promote Peace… One School at a Time*, the subtitle of the hardback version reads, *One Man's Mission to Fight Terrorism and Build Nations… One School at a Time*. Mortenson has written a new book that was released in December 2009: Stones into Schools: Promoting Peace with Books, Not Bombs, in Afghanistan and Pakistan (Mortenson & Bryan, 2009).

References

Abuza, Z. (2003). *Militant Islam in Southeast Asia: Crucible of Terror*. Boulder, CO: Lynne Reinner Publishers.

Anonymous (2009). "Deception 2.0: Deceiving in the Netwar Age." Unpublished Paper. Task Force Iron, Iraq.

Arreguin-Toft, I. (2001). "How the Weak Win Wars: A Theory of Asymmetric Conflict." *International Security* 26, 1: 93-128.

Arreguin-Toft, I. (2005). *How the Weak Win Wars: A Theory of Asymmetric Conflict*. Cambridge, UK: Cambridge University Press.

Asal, V., & Rethemeyer, R. K. (2006). "Researching Terrorist Networks." *Journal of Security Education* 1, 4: 65-74.

Asal, V., & Rethemeyer, R. K. (2008). "The Nature of the Beast: Organizational Structures and the Lethality of Terrorist Attacks." *The Journal of Politics* 70, 2: 437-449.

Azarian, G. R. (2005). *The General Sociology of Harrison C. White: Chaos and Order in Networks*. New York: Palgrave Macmillan.

Baker, W. E., & Faulkner, R. R. (1993). The Social-Organization of Conspiracy: Illegal Networks in the Heavy Electrical-Equipment Industry. *American Sociological Review* 58, 6: 837-860.

Banlaoi, R. C. (2009). *Counter Terrorism Measures in Southeast Asia: How Effective Are They?* Manilla, Philippines: Yuchengco Center: De La Salle University.

Batagelj, V., & Mrvar, A. (2010). *Pajek 1.27*. Lubjlijana, Slovenia: University of Ljubljana.

Borgatti, S. P. (2006). "Identifying Sets of Key Players in a Social Network." *Computational, Mathematical and Organizational Theory* 12: 21-34.

Borgatti, S. P., Carley, K. M., & Krackhardt, D. (2006). "On the Robustness of Centrality Measures under Conditions of Imperfect Data." *Social Networks* 28: 124-136.

Boucek, C. (2008a). "The Sakinah Campaign and Internet Counter-Radicalization in Saudi Arabia." *CTC Sentinel* 1, 9: 1-4. Available: http://carnegieendowment.org/files/CTCSentinel_Vol1Iss9.pdf [January 5, 2011].

Boucek, C. (2008b). "Saudi Arabia's 'Soft' Counterterrorism Strategy: Prevention, Rehabilitation, and Aftercare." *Carnegie Papers*, No. 97. Available: http://carnegieendowment.org/files/cp97_boucek_saudi_final.pdf [January 5, 2011].

Breiger, R. L. (1975). "Dual and Multiple Networks of Social Structures: A Study of Affiliation and Interaction." Unpublished Doctoral Dissertation, Harvard University, Boston.

Brimley, S., & Singh, V. (2008). "Stumbling into the Future? The Indirect Approach and American Strategy." *Orbis* 52, 2: 312-331.

Cooper, H. (2009). "Dreaming of Splitting the Taliban." *The New York Times*. Available: http://www.nytimes.com/2009/03/08/weekinreview/08COOPER.html?_r=1 [January 5, 2011].

Davis, L. E., & Sisson, M. W. (2009). *A Strategic Planning Approach: Defining Alternative Counterterrorism Strategies as an Illustration*. Santa Monica, CA: RAND Corporation.

de Nooy, W., Mrvar, A., & Batagelj, V. (2005). *Exploratory Social Network Analysis with Pajek*. Cambridge, UK: Cambridge University Press.

Diani, M., & McAdam, D. (Eds.). (2003). *Social Movements and Networks: Relational Approaches to Collective Action*. Oxford and New York: Oxford University Press.

Doreian, P., Batagelj, V., & Ferligoj, A. (2005). *Generalized Blockmodeling*. New York and Cambridge: Cambridge University Press.

Ettlinger, N., & Bosco, F. (2004). "Thinking through Networks and their Spatiality: A Critique of the U.S. (Public) War on Terrorism and its Geographic Discourse." *Antipode* 36, 2: 249-271.

Everton, S. F. (Forthcoming). "Network Topography, Key Players and Terrorist Networks." *Connections*.

Felter, J., & Fishman, B. (2007). "Al-Qa'ida's Foreign Fighters in Iraq: A First Look at the Sinjar Records." Available: http://www.ctc.usma.edu/harmony/pdf/CTCForeignFighter.19.Dec07.pdf [January 5, 2011].

Fink, N. C., & Hearne, E. B. (2008). "Beyond Terrorism: Deradicalization and Disengagement from Violent Extremism." Available: http://www.ipacademy.org/media/pdf/publications/beter.pdf [January 5, 2011].

Flynn, M. T., Pottinger, M., & Batchelor, P. D. (2010). *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan*. Washington DC: Center for a New American Security.

Fridovich, D. P., & Krawchuk, F. T. (2007). "Special Operations Forces: Indirect Approach." *Joint Forces Quarterly* 44, 1: 24-27.

Granovetter, M. (1973). "The Strength of Weak Ties." *American Journal of Sociology* 73, 6: 1360-1380.

Horgan, J. (2009). *Walking Away from Terrorism: Accounts of Disengagement from Radical and Extremist Movements*. New York: Routledge.

International Crisis Group (2006). *Terrorism in Indonesia: Noordin's Networks* (No. Asia Report #114). Brussels, Belgium: International Crisis Group.

International Crisis Group (2008). *Indonesia: Jemaah Islamiyah's Publishing Industry*. Brussels, Belgium: International Crisis Group.

Jones, S. G., & Libicki, M. C. (2008). *How Terrorist Groups End: Lessons for Countering al Qa'ida*. Santa Monica, CA: RAND Corporation.

Jordan, J., Mañas, F. M., & Horsburgh, N. (2008). "Strengths and Weaknesses of Grassroot Jihadist Networks: The Madrid Bombings." *Studies in Conflict & Terrorism* 31: 17-21.

Keefe, P. (2006). "Can Network Theory Thwart Terrorists?" *The New York Times*. Available: http://www.nytimes.com/2006/03/12/magazine/312wwln_essay.html [January 5, 2011].

Krawchuk, F. T. (ND). "Winning the Global War on Terrorism in the Pacific Region: Special Operations Forces' Indirect Approach to Success." Available: http://igcc.ucsd.edu/research/security/DACOR/presentations/krawchuk.pdf [January 5, 2011].

Krebs, V. (2001). "Mapping Networks of Terrorist Cells." *Connections* 24, 3: 43-52.

Lempert, R. J., Trujillo, H. R., Aaron, D., Dewar, J. A., Berry, S. H., & Popper, S. W. (2008). "Comparing Alternative U.S. Counterterrorism Strategies: Can Assumption-Based Planning Help Elevate the Debate?" Available: http://www.rand.org/pubs/documented_briefings/2008/RAND_DB548.pdf [January 5, 2011; large document].

Lum, C., Kennedy, L. W., & Sherley, A. J. (2006). The Effectiveness of Counter-Terrorism Strategies. *Campbell Systematic Reviews* 2006, 2: 51. Available: http://www.rutgerscps.org/publications/Lum_Terrorism_Review.pdf [January 5, 2011].

Lum, T., & Niksch, L. A. (2006; updated 2009). "The Republic of the Philippines: Background and U.S. Relations: Congressional Research Service Report to Congress." Available: http://www.fas.org/sgp/crs/row/RL33233.pdf [January 5, 2011].

Magouirk, J., Atran, S., & Sageman, M. (2008). "Connecting Terrorist Networks." *Studies in Conflict & Terrorism* 31: 1-16.

Marks, S., Meer, T., & Nilson, M. (2005). "Manhunting: A Methodology for Finding Persons of National Interest." Unpublished Master of Science, Naval Postgraduate School, Monterey, CA.

McAdam, D. (1982). *Political Process and the Development of Black Insurgency, 1930-1970*. Chicago: University of Chicago Press.

McAdam, D. (1999). *Political Process and the Development of Black Insurgency, 1930-1970* (2nd ed.). Chicago: University of Chicago Press.

McCarthy, J. D., & Zald, M. N. (1977). "Resource Mobilization and Social Movements: A Partial Theory." *American Journal of Sociology* 82, 6: 1212-1241.

Moody, J. (2005). Fighting a Hydra: A Note on the Network Embeddedness of the War on Terror. *Structure and Dynamics* 1, 2. Available: http://escholarship.org/uc/item/7x3881bs [January 5, 2011].

Moon, I.-C. (2008). "Destabilization of Adversarial Organizations with Strategic Interventions." Unpublished Doctoral Thesis, Carnegie Mellon University, Pittsburgh, PA. Available: http://www.casos.cs.cmu.edu/publications/papers/CMU-ISR-08-124.pdf [January 5, 2011].

Mortenson, G., & Bryan, M. (2009). *Stones into Schools: Promoting Peace with Books, Not Bombs, in Afghanistan and Pakistan*. New York: Viking.

Mortenson, G., & Relin, D. O. (2006). *Three Cups of Tea: One Man's Mission to Fight Terrorism and Build Nations... One School at a Time*. New York: Viking.

Pedahzur, A., & Perliger, A. (2006). "The Changing Nature of Suicide Attacks: A Social Network Perspective." *Social Forces* 84, 4: 1987-2008.

Peter, T. A. (2008). "U.S. Begins Hunting Iraq's Bombmakers, Not Just Bombs." *The Christian Science Monitor*. Available: http://www.csmonitor.com/2008/0908/p04s01-wome.html [January 5, 2011].

Popielarz, P. A., & McPherson, J. M. (1995). "On the Edge or in Between: Niche Position, Niche Overlap, and the Duration of Voluntary Association Memberships." *American Journal of Sociology* 101, 3: 698-720.

Raab, J., & Milward, H. B. (2003). "Dark Networks as Problems." *Journal of Public Administration Research and Theory* 13, 4: 413-439.

Rabasa, A. (2005). "Islamic Education in Southeast Asia." In H. Fradkin, H. Haqqani & E. Brown (Eds.), *Current Trends in Islamist Ideology* (pp. 97-108). Washington, D.C.: Hudson Institute.

Ramakrishna, K. (2005). "Delegitimizing Global Jihadi Ideology in Southeast Asia." *Contemporary Southeast Asia* 27, 3: 343-369.

Rodriguez, J. A. (2005). *The March 11th Terrorist Network: In Its Weakness Lies Its Strength*. Barcelona, Spain: Departament de Sociologia i Anàlisi de les Organitzacions: Universitat de Barcelona.

Sageman, M. (2004). *Understanding Terror Networks*. Philadelphia, PA: University of Pennsylvania Press.

Schmitt, E., & Perlez, J. (2009). "Strikes Worsen Qaeda Threat, Pakistan Says." *The New York Times*. Available: http://www.nytimes.com/2009/02/25/world/asia/25drones.html?scp=1&sq=Schmitt%20and%20Perlez,%202009&st=cse [January 5, 2011].

Simmel, G. ([1908, 1922] 1955). *Conflict & The Web of Group-Affiliations* (K. H. Wolff & R. Bendix, Trans.). New York: The Free Press.

Smith, C. S. (1991). *The Emergence of Liberation Theology: Radical Religion and Social Movement Theory*. Chicago: University of Chicago Press.

Smith, C. S. (1996). *Resisting Reagan: The U.S. Central America Peace Movement*. Chicago: The University of Chicago Press.

Sparrow, M. K. (1991). "The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects." *Social Networks* 13: 251-274.

Stark, R., & Bainbridge, W. S. (1980). "Networks of Faith: Interpersonal Bonds and Recruitment to Cults and Sects." *American Journal of Sociology* 85, 6: 1376-1395.

Tsvetovat, M., & Carley, K. M. (2005). "Structural Knowledge and Success of Anti-Terrorist Activity: The Downside of Structural Equivalence." *Journal of Social Structure* 6, 2. Available: http://www.cmu.edu/joss/content/articles/volume6/TsvetovatCarley/index.html [January 5, 2011].

U.S. Army (2007). *U.S. Army/Marine Counterinsurgency Field Manual* (FM 3-24). Old Saybrook, CT: Konecky & Konecky.

U.S. Director of Operations (2006). *Information Operations: Joint Publication 3-13*. Available: http://www.fas.org/irp/doddir/dod/jp3_13.pdf [January 5, 2011].

U.S. Special Operations Command (2003). *Doctrine for Joint Psychological Operations: Joint Publication 3-53*. Available: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB177/02_psyop-jp-3-53.pdf [January 5, 2011].

van Meter, K. M. (2001). "Terrorists/Liberators: Researching and Dealing with Adversary Social Networks." *Connections* 3: 66-78.

White, H. C. (2008). *Identity and Control: How Social Formations Emerge* (2nd ed.). Princeton, NJ: Princeton University Press.

Wikipedia (2010). "Noordin Mohammed Top." Available: http://en.wikipedia.org/wiki/Noordin_Mohammad_Top [January 5, 2011].

Wiktorowicz, Q. (2004). "Introduction: Islamic Activism and Social Movement Theory." In Q. Wiktorowicz (Ed.), *Islamic Activism: A Social Movement Theory Approach* (pp. 1-33). Bloomington: Indiana University Press.

Wilson, G. (2006). "Anatomy of a Successful COIN Operation: OEF-Philippines and the Indirect Approach." *Military Review* (November-December): 2-12. Available: http://usacac.army.mil/CAC2/MilitaryReview/Archives/English/MilitaryReview_2008CRII0831_art009.pdf [January 5, 2011].